

Vertrag zur Auftragsverarbeitung gemäss Art. 28 DSGVO

Zwischen der Firma

Institut für angewandte Morphologie GmbH (kurz IAM)

c/o SokratesGroup

Glärnischstrasse 16

CH 8803 Rüschlikon

– nachfolgend „**Auftragnehmer**“ genannt –

und der Firma

– nachfolgend „**Auftraggeber**“ genannt –

besteht / bestehen unter

Kundennummer / Vertrags- / Offert-Datum

ein / mehrere von dem Auftraggeber genutzte(r) Vertrag / Verträge.

HINWEIS: Dieser Auftragsverarbeitungsvertrag regelt die Verarbeitung der Daten des Auftraggebers durch den Auftragnehmer im Sinne des Art. 28 der EU Datenschutz-Grundverordnung (DSGVO) sowie im Sinne des Art. 9 des Schweizerischen Bundesgesetzes über den Datenschutz (DSG).

1. Gegenstand dieses Auftragsverarbeitungsvertrages (Art. 28 Abs. 1 DSGVO)

1.1 Gegenstand des Vertrages ist die Bereitstellung von Webhosting-Dienstleistungen bzw. eines (oder mehrerer) dedizierten/dedizierter Webserver(s) sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung, SokratesMap-Applikationen, etc.. Im Rahmen dieses Vertrages hat der Auftraggeber – je nach Tarif und vereinbartem Leistungsumfang – unter Nutzung u.a. z.B. eines Webserver, FTP-Servers oder ssh-Zugangs die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen).

1.1.1 Das IAM führt selbst keine IT-Leistungen oder Datenverarbeitungen durch, sondern kauft diese Leistungen bei Subunternehmen ein, vgl. Anhang.

1.2 Gegenstand des Vertrages ist **nicht** die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers in Zusammenarbeit mit vorerwähnten IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

1.3 Die Einzelheiten ergeben sich aus dem Hauptvertrag / den Hauptverträgen, die unter der benannten Kundennummer zusammengefasst sind. Die Vereinbarung zur Auftragsverarbeitung findet Anwendung auf das gesamte Dienstleistungsverhältnis, sofern die in Punkt 1.1 beschriebenen Dienstleistungen betroffen sind.

1.3.1 Die SokratesMap-Applikation: Diese ist nicht originär zur Bearbeitung und Speicherung von Personendaten vorgesehen. Der Auftragnehmer weist ausdrücklich darauf hin, dass mit den SokratesMaps keine Personenprofile erstellt werden dürfen, sondern lediglich Organisationen / Projekte / Rollen / Stellen abgebildet werden dürfen, die dann in ausgedruckter Form personalisiert und entsprechend DSGVO-konform behandelt werden müssen.

1.4 Soweit nachfolgend von Daten die Rede ist, handelt es sich ausschliesslich um (nicht?)-personenbezogene Daten im Sinne der DSGVO. Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung i.S.d. Art. 28 Abs. 1 DSGVO, die der Auftragnehmer gegenüber dem Auftraggeber erbringt und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1.5 In **Ergänzung** zu dem/den zwischen den Parteien geschlossenen Vertrag/Verträgen konkretisieren die Vertragsparteien mit vorliegendem Auftragsverarbeitungsvertrag die gegenseitigen Pflichten im generellen Umgang mit den Daten des Auftraggebers.

2. Laufzeit, Beendigung, Löschung von Daten (Art. 28 Abs. 1 DSGVO)

2.1 Die Laufzeit des Vertrages richtet sich nach der Dauer der Erbringung von SokratesMaps, bzw. Hosting-Leistungen des Auftragnehmers an den Auftraggeber. Der Auftrag endet, wenn der Auftraggeber keine SokratesMaps- / Hosting-Leistungen des Auftragnehmers, entsprechend den Leistungsvereinbarungen/Angeboten der einzelnen Auftragsbestätigungen für SokratesMap- / Hosting-Leistungen des Auftragnehmers, mehr in Anspruch nimmt.

2.2 Die Rechte der durch den Datenumgang bei dem Auftragnehmer betroffenen Personen, insbesondere auf Berichtigung, Löschung und Sperrung, sind gegenüber dem Auftraggeber geltend zu machen. Der Auftraggeber ist allein verantwortlich für die Wahrung dieser Rechte.

2.3 Nach Ende des Auftrags oder auf schriftliche Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche Daten des Auftraggebers vollständig datenschutzgerecht zu löschen (einschliesslich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder an den Auftraggeber zurückzugeben, wobei die SokratesMaps (auch im Sinne des geistigen Eigentums?) im Eigentum des Auftragnehmers verbleiben. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Dies gilt nicht für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemässen Datenverarbeitung dienen oder soweit z.B. rechtliche Regelungen, gesetzliche Pflichten oder gerichtliche Verfügungen dem entgegenstehen. Entstehen durch eine Löschung vor Vertragsbeendigung zusätzliche Kosten, so trägt diese der Auftraggeber.

2.4 Der Auftragnehmer ist verpflichtet, im Rahmen seiner Tätigkeit für den Auftraggeber an ihn gerichtete Ersuchen Betroffener zur sachgerechten Bearbeitung unverzüglich an die Auftraggeber weiterzuleiten. Er ist nicht berechtigt, diese Ersuchen ohne Abstimmung mit dem Auftraggeber selbständig zu bescheiden.

2.5 Der Auftragnehmer hat den Auftraggeber bei der Umsetzung der Rechte der Betroffenen nach Kapitel III der DSGVO, insbesondere im Hinblick auf Berichtigung, Sperrung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen der technischen Möglichkeiten, insbesondere hinsichtlich des Charakters der geschuldeten Dienstleistung, zu unterstützen.

2.6 Zu einem Datenträgeraustausch gemäss Art. 28 Abs. 3 lit. g DSGVO zwischen den Beteiligten dieser Auftragsverarbeitung kommt es nicht. Insoweit ist eine Rückgabe nicht zu regeln.

3. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten

3.1 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Vertragsparteien bestehenden Vertrag.

Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschliesslich zur vertraglich vereinbarten Leistung zu verwenden. Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemässen Erhebung, Verarbeitung und / oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. Dem Auftragnehmer ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmässigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Auftraggeber verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschl. Marketingzwecke, sind nicht gestattet.

3.2 Soweit seitens des Auftragnehmers eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, geschieht dies im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in Drittländern, sofern die besonderen Voraussetzungen der DSGVO eingehalten werden.

4. Art der Daten und Kreis der Betroffenen (Art. 28 Abs. 3 S. 1 DSGVO)

4.1 Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung der Daten des Auftraggebers gem. Ziff.

1.2 Satz 2 sind folgende Datenarten:

(durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen!)

- Personenstammdaten (entfällt)
- Kommunikationsdaten (z.B. Telefon, E-Mail) (entfällt)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) (entfällt)
- Kundenhistorie (entfällt)
- Vertragsabrechnungs- und Zahlungsdaten (entfällt)
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen) (entfällt)
- Sonstige Daten: Erfassen der vom Auftraggeber autorisierten User mit Vorname und Nachname.

4.2 Kreis der Betroffenen

Der Kreis der durch den Umgang mit den Daten gem. Ziff. 1.2 Satz 2 Betroffenen umfasst: *(durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen!)*

- Kunden (entfällt)
- Interessenten (entfällt)
- Abonnenten (entfällt)
- Beschäftigte (entfällt)
- Lieferanten (entfällt)
- Handelsvertreter (entfällt)
- Ansprechpartner (entfällt)
- Sonstige Betroffene: (entfällt)

5. Pflichten des Auftragnehmers

5.1 Allgemeine Pflichten Art. 28-33 DSGVO

5.1.1 Der Auftragnehmer (das Institut für angew. Morphologie GmbH) verpflichtet sich zu einer schriftlichen Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäss Art. 37, 38 DSGVO ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber auf Anforderung, zum Zweck der direkten Kontaktaufnahme, mitgeteilt.

5.1.2 Soweit seitens des Auftragnehmers eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, ist dies nur zulässig im Rahmen der vertraglichen Vereinbarungen zwischen Auftraggeber und Auftragnehmer. Soweit der Auftragnehmer Zugriff auf Daten des Auftraggebers hat, verwendet er diese nicht für vertragsfremde Zwecke, insbesondere gibt er diese an Dritte nur weiter, soweit hierzu eine gesetzliche Verpflichtung besteht. Kopien von Daten dürfen nur mit Zustimmung des Auftraggebers erstellt werden. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemässen Datenverarbeitung oder Erfüllung vertraglicher oder gesetzlicher Verpflichtungen erforderlich sind.

5.1.3 Der Auftragnehmer stellt die Wahrung der Vertraulichkeit entsprechend Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO sicher. Alle Personen, die auftragsgemäss auf die unter Punkt 4.1 aufgeführten Daten des Auftraggebers zugreifen können, müssen auf die Vertraulichkeit verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

5.1.4 Der Auftragnehmer stellt die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Massnahmen entsprechend Art. 32 DSGVO sicher.

5.1.5 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei von ihm oder der bei ihm beschäftigten Personen begangenen Verstössen gegen Datenschutzvorschriften. Gleiches gilt im Falle schwerwiegender Störungen des Betriebsablaufs oder anderen Unregelmässigkeiten im Umgang mit Daten des Auftraggebers. Soweit den Auftraggeber Pflichten nach Art. 32 und 33 DSGVO treffen, hat der Auftragnehmer ihn hierbei zu unterstützen. Soweit den Auftraggeber Pflichten nach Art. 32-36 DSGVO treffen, z.B. im Falle des Abhandenkommens oder der unrechtmässigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten durch Dritte, hat der Auftragnehmer ihn hierbei im Rahmen des Charakters der durch den Auftragnehmer erbrachten Dienstleistung zu unterstützen.

5.2 Technische und organisatorische Massnahmen (Art. 32 DSGVO)

5.2.1 Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft dabei technische und organisatorische Massnahmen zur angemessenen Sicherung der Daten vor Missbrauch und Verlust,

um den Anforderungen der DSGVO zu entsprechen.

5.2.2 Die Parteien sind sich einig, dass die technischen und organisatorischen Massnahmen dem technischen Fortschritt und der Weiterentwicklung unterliegen. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Massnahmen umzusetzen. Er muss den Auftraggeber hierüber auf Anfrage informieren und sicherstellen, dass das Sicherheitsniveau der festgelegten Massnahme nicht unterschritten wird. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Massnahmen um Massnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Wesentliche Änderungen sind zu dokumentieren.

6. Unterauftragsverhältnisse (Art. 28 Abs. 2 u. 4 DSGVO)

6.1 Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen, insbesondere, aber nicht ausschliesslich, für die Bereiche Wartung und Installation der Rechenzentrumsinfrastruktur, Telekommunikationsdienstleistungen und Benutzerservice, verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt. Der Auftragnehmer behält sich vor, gemäss Ziffer 3.2 dieser Vereinbarung Subunternehmer in den dort genannten Regionen einzusetzen.

6.2 Der Auftragnehmer trägt dafür Sorge, dass dem Auftraggeber eine aktuelle Liste der eingesetzten Unterauftragnehmer im Kundenportal, als Anhang zu dieser Vereinbarung oder auf sonstige Weise stets zum Abruf und Einsicht zur Verfügung steht, diese ist fester Bestandteil der vorliegenden Vereinbarung. Der Auftraggeber stimmt dem Einsatz der dort genannten Subunternehmer zu. Bei Änderung dieser Liste in Bezug auf die Hinzuziehung oder Ersetzung von weiteren Subunternehmern ergeht hierüber eine Information an den Auftraggeber. Die Änderungen gelten als vom Auftraggeber akzeptiert, wenn dieser nicht innerhalb von 4 Wochen nach Veröffentlichung widerspricht.

6.3 Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Auftragsverarbeitungsvertrag dem Unterauftragnehmer zu übertragen.

7. Pflichten des Auftraggebers (Art. 24 DSGVO und Art. 13 und 14 DSGVO)

7.1 Der Auftraggeber ist für die Einhaltung der für ihn einschlägigen datenschutzrechtlichen Regelungen verantwortlich.

7.2 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er Verstösse des Auftragnehmers gegen datenschutzrechtliche Bestimmungen feststellt.

7.3 Den Auftraggeber treffen die sich aus Art. 24 DSGVO und Art. 13 und 14 DSGVO ergebenden Informationspflichten.

8. Weisungsbefugnisse, Berichtigung, Löschung und Sperrung, Rechte Betroffener (Art. 29 i.V.m. 28 DSGVO sowie Kapitel III der DSGVO)

8.1 Der Auftraggeber hat selbst jederzeit umfassenden Zugriff auf die Daten, so dass es einer Mitwirkung des Auftragnehmers insbesondere auch zu Berichtigung, Sperrung, Löschung etc. nicht bedarf. Soweit eine Mitwirkung des Auftragnehmers erforderlich ist, ist der Auftragnehmer hierzu gegen Erstattung der anfallenden Kosten verpflichtet. Dem Auftraggeber steht in diesem Fall ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung gemäss Art. 29 i.V.m. 28 DSGVO zu. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

8.2 Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten. Ist der Auftraggeber auf Grund geltender Datenschutzgesetze verpflichtet, Auskünfte zur Erhebung, Verarbeitung und / oder Nutzung von Daten zu erteilen, wird der Auftragnehmer den Auftraggeber dabei soweit notwendig bei der Bereitstellung dieser Informationen unterstützen. Eine diesbezügliche Anfrage hat der Auftraggeber schriftlich an den Auftragnehmer zu richten und diesem die hierdurch entstandenen Kosten zu erstatten.

9. Kontrollrechte des Auftraggebers

9.1 Der Auftraggeber hat das Recht, sich vor Beginn der Datenverarbeitung und sodann regelmässig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Massnahmen zu überzeugen.

9.2. Dem Auftraggeber steht hierzu die durch den Datenschutzbeauftragten des Auftragnehmers erstellte, regelmässig überarbeitete und den gesetzlichen Anforderungen entsprechende Dokumentation über die vorhandenen technischen und organisatorischen Massnahmen zur Verfügung.

9.3. Der Auftraggeber hat das Recht, die Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, nach rechtzeitiger vorheriger Anmeldung (3 Wochen) zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in seinem Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Kosten, die dem Auftragnehmer durch seine Unterstützungshandlung entstehen, sind ihm im angemessenen Umfang zu erstatten.

9.4 Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach Art. 28 Abs. 1 DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass der Auftraggeber sich von der Einhaltung der getroffenen technischen und organisatorischen Massnahmen überzeugen kann.

9.5 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner bei der Verarbeitung der oben genannten Daten bestehende Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und Nachweise zu führen. Dies gilt auch, soweit der Auftragnehmer die Kontrolle seiner Unterauftragnehmer für den Auftraggeber durchführt.

10. Salvatorische Klausel, Gerichtsstand

10.1 Sollte eine Bestimmung dieses Vertrages ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrages hiervon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.

10.2 Als Gerichtsstand wird der Hauptsitz des Instituts für angewandte Morphologie GmbH vereinbart.

, den

Unterschrift des Auftraggeber

Auftragnehmer Institut für angewandte Morphologie GmbH

Anlage:

Technische und organisatorische Massnahmen:

Vorgesehen:
Informale Anwendung von ISO 27001 - Self Assessment

Bestellung des Datenschutzbeauftragten:

Benjamin Jenni
Managing Partner
SokratesGroup
Tel. +41 44 724 2011
Mail: benjamin.jenni@sokratesgroup.com

Liste der Subunternehmer

Programmierung und Betrieb der Applikation "SokratesMapConcept":

P-soft GmbH
Gartenweg 14
CH-5080 Laufenburg

Durchführung / Betrieb der Applikation im Auftrag der Firma P-soft:

Host Europe GmbH
c/o WeWork
Friesenplatz 4
D-50672 Köln